PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

#4

Ryu INADA et al. Group Art Unit: 2152

Application No.: 09/987,41[illegible]

Filed: November 14, 2001 Docket No.: 111121

For: METHOD AND APPARATUS FOR PROCESSING SUBJECT NAME INCLUDED IN PERSONAL CERTIFICATE

CLAIM FOR PRIORITY

Director of the U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

The benefit of the filing dates of the following prior foreign applications filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:

Japanese Patent Application No. 2001-315276 filed October 12, 2001
Japanese Patent Application No. 2000-350185 filed November 16, 2000
In support of this claim, certified copies of said original foreign applications:

__X__ are filed herewith.

_____ were filed on _____ in Parent Application No. _____ filed _____.

_____ will be filed at a later date.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of these documents.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Joel S. Armstrong
Registration No. 36,430

JAO:JSA/mlb

Date: December 26, 2001

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年１０月１２日

出願番号
Application Number: 特願２００１－３１５２７６

出願人
Applicant(s): 富士ゼロックス株式会社

２００１年１２月　７日

特許庁長官
Commissioner,
Japan Patent Office　及川耕造

出証番号　出証特２００１－３１０６９００

【書類名】　特許願

【整理番号】　FE01-01395

【提出日】　平成13年10月12日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/60

【発明の名称】　個人証明書サブジェクト名処理装置および方法

【請求項の数】　19

【発明者】

【住所又は居所】　神奈川県川崎市高津区坂戸３丁目２番１号　ＫＳＰ　Ｒ＆Ｄ　ビジネスパークビル　富士ゼロックス株式会社内

【氏名】　稲田　龍

【発明者】

【住所又は居所】　神奈川県川崎市高津区坂戸３丁目２番１号　ＫＳＰ　Ｒ＆Ｄ　ビジネスパークビル　富士ゼロックス株式会社内

【氏名】　黒崎　雅人

【特許出願人】

【識別番号】　000005496

【氏名又は名称】　富士ゼロックス株式会社

【電話番号】　0462-38-8516

【代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100093241

【弁理士】

【氏名又は名称】　宮田　正昭

【選任した代理人】

【識別番号】　100101801

【弁理士】

【氏名又は名称】　山田　英治

【先の出願に基づく優先権主張】

【出願番号】　特願2000-350185

【出願日】　平成12年11月16日

【手数料の表示】

【予納台帳番号】　038818

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9605865

【包括委任状番号】　0006675

【包括委任状番号】　0006676

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　個人証明書サブジェクト名処理装置および方法

【特許請求の範囲】

【請求項１】　個人証明書に含まれるサブジェクト名を処理する個人証明書サブジェクト名処理装置において、

個人証明書を受信する手段と、

受信した個人証明書を電子署名技術に基づいて検証する手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも１つの所定のエレメントを抽出する手段と、

上記検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定する手段とを有することを特徴とする個人証明書サブジェクト名処理装置。

【請求項２】　上記所定のエレメントのうちの１つは、上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームである請求項１記載の個人証明書サブジェクト名処理装置。

【請求項３】　上記所定のエレメントは、業務のプロジェクト名を表すために割り当てられた１の階層のオーガニゼーショナル・ユニット・ネームと、目的を表すために割り当てられた、コモンネームの一部とする請求項１記載の個人証明書サブジェクト名処理装置。

【請求項４】　個人証明書を受信する手段と、

受信した個人証明書を電子署名技術に基づいて検証する手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも１つの所定のエレメントを抽出する手段と、

受信した個人証明書の検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定する手段とを有することを特徴とするウェブ・サーバ・コンピュータ・システム。

【請求項５】　個人証明書を受信する手段と、

受信した個人証明書を電子署名技術に基づいて検証する手段と、

受信した個人証明書の検証が成功したときに、セッション識別子を割り当てる

手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも１つの所定のエレメントを抽出する手段と、

受信した個人証明書の検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定する手段と、

決定したアクセス権限を上記セッション識別子に関連づけて保持する手段とを有することを特徴とするウェブ・サーバ・コンピュータ・システム。

【請求項６】　上記所定のエレメントのうちの１つは、上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームである請求項５記載のウェブ・サーバ・コンピュータ・システム。

【請求項７】　上記所定のエレメントは、業務のプロジェクト名を表すために割り当てられた１の階層のオーガニゼーショナル・ユニット・ネームと、目的を表すために割り当てられた、コモンネームの一部とする請求項５記載のウェブ・サーバ・コンピュータ・システム。

【請求項８】　サブジェクト名の所定のエレメントが保持者の所属組織および個人ＩＤ以外の属性を表す個人証明書を受信して当該サブジェクト名を処理する個人証明書サブジェクト名処理装置において、

上記個人証明書を受信する手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出する手段と、

少なくとも、上記所定のエレメントの値が表す、保持者の所属組織および個人ＩＤ以外の属性に基づいて、アクセス権限を決定する手段とを有することを特徴とする個人証明書サブジェクト名処理装置。

【請求項９】　上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、保持者がオーガニゼーション・ネームが表す組織の構成員ではなく、かつ当該組織に対して協力していることを示す請求項８記載の個人証明書サブジェクト名処置装置。

【請求項１０】　上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、保持者が参加するプロジェクト名を表す請求項８記載の個

人証明書サブジェクト名処理装置。

【請求項１１】　上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、オーガニゼーション・ネームが表す組織に対して協力し、かつ保持者が属する、協力組織名を表す請求項８記載の個人証明書サブジェクト名処理装置。

【請求項１２】　上記サブジェクト名の所定階層のオーガニゼーショナル・ユニット・ネームが、保持者が参加する業務の種類を表す請求項８記載の個人証明書サブジェクト名処理装置。

【請求項１３】　上記サブジェクト名のコモンネームが、保持者が参加する業務の種類を表す請求項８記載の個人証明書サブジェクト名処理装置。

【請求項１４】　個人証明書を受信する手段と、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出する手段と、

上記所定のエレメントの値に基づいてアクセス権限を決定する手段とを有することを特徴とする個人証明書サブジェクト名処理装置。

【請求項１５】　個人証明書に含まれるサブジェクト名を処理する個人証明書サブジェクト名処理方法において、

個人証明書を受信するステップと、

受信した個人証明書を電子署名技術に基づいて検証するステップと、

受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも１つの所定のエレメントを抽出するステップと、

上記検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定するステップとを有することを特徴とする個人証明書サブジェクト名処理方法。

【請求項１６】　サブジェクト名の所定のエレメントが保持者の所属組織および個人ＩＤ以外の属性を表す個人証明書を受信して当該サブジェクト名を処理する個人証明書サブジェクト名処理方法において、

上記個人証明書を受信するステップと、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを

抽出するステップと、

少なくとも、上記所定のエレメントの値が表す、保持者の所属組織および個人ＩＤ以外の属性に基づいて、アクセス権限を決定するステップとを有することを特徴とする個人証明書サブジェクト名処理方法。

【請求項１７】　個人証明書に含まれるサブジェクト名を処理するためにコンピュータに用いられる個人証明書サブジェクト名処理用コンピュータ・プログラムにいて、

個人証明書を受信するステップと、

受信した個人証明書を電子署名技術に基づいて検証するステップと、

受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも１つの所定のエレメントを抽出するステップと、

上記検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定するステップとをコンピュータに実行させるために用いられることを特徴とする個人証明書サブジェクト名処理用コンピュータ・プログラム。

【請求項１８】　サブジェクト名の所定のエレメントが保持者の所属組織および個人ＩＤ以外の属性を表す個人証明書を受信して当該サブジェクト名を処理するためにコンピュータに用いられる個人証明書サブジェクト名処理用コンピュータ・プログラムにおいて、

上記個人証明書を受信するステップと、

受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出するステップと、

少なくとも、上記所定のエレメントの値が表す、保持者の所属組織および個人ＩＤ以外の属性に基づいて、アクセス権限を決定するステップとをコンピュータに実行させるために用いられることを特徴とする個人証明書サブジェクト名処理用コンピュータ・プログラム。

【請求項１９】　サブジェクト名のオーガニゼーショナル・ユニット・ネームおよびコモン・ネームの少なくとも１つが保持者の所属組織および個人ＩＤ以外の属性を表す個人証明書を記録したコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、個人証明書（以下では単に証明書と呼ぶこともある）のサブジェクト名を利用してアクセスを制御する技術に関する。

【０００２】

【従来の技術】

ＩＴＵ－Ｔ勧告Ｘ．５０９はディレクトリモデル認証を規定しており、このディレクトリモデル認証に準拠して個人証明書を発行局（認証局）から発行してもらう。発行局は申請人から証明書の発行に必要な情報（名前、所属、公開鍵等）を受け取り所定のポリシーに従い証明書を発行し、証明書を所定の証明書格納部に保存する。申請人は証明書格納部から証明書を取り出すことができる。

【０００３】

ところで、個人証明書のサブジェクト名を見ただけでは、その証明書の保持者がどういう権限を有しており、どういう性質をもっているか不明である。保持者が有している権限や性質を知るために種々のアプローチが採用されている。例えば、証明書のサブジェクト名と権限とをデータベースに登録し、証明書を用いたアクセスがあるたびにデータベースに問合せる。しかしこの方法は効率の面で問題があった。

【０００４】

図１０は、上述の従来のアプローチを実現するシステム例を示している。この図において、ユーザはクライアント端末５００を用いてネットワーク（例えばインターネット）５０１を介してウェブ・サーバ５０２にアクセスする。このアクセスはＳＳＬ手法を用いて行われ、クライアント端末５００およびウェブ・サーバ５０２の間で証明書を交換し、認証を行い、この後、ネゴシエーションにより決定された慣用暗号によりデータを暗号化して送受信する。ウェブ・サーバ５０２は、クライアント端末５００から送られた証明書のサブジェクト名（証明書に記載されている被認証者の識別子）を用いてデータベースサーバ（ディレクトリサービス）５０３に問い合わせクライアント端末５００のユーザがアクセス権限

を有するかどうかを知る。例えば、アクセス対象の権限レベル（例えば０、１、２等）とサブジェクト名を引数としてデータベースサーバ５０３に問い合わせ、当該サブジェクト名のユーザが当該権限レベルにアクセスできるかどうかを応答として受け取る。データベースサーバ５０３は、ユーザ（サブジェクト名）と許容されている権限レベルとの関係を記憶保持している。もちろん、サブジェクト名を引数として許容権限レベルを受け取ってウェブ・サーバ５０２側においてアクセス対象ファイルがその許容権限レベル以内かを判別するようにすることもあるし、サブジェクト名とアクセス対象ファイル名（ディレクトリ名）をデータベースサーバ５０３に引き渡して照会を行ってもよい。

【０００５】

以上のような従来のアプローチでは、アクセスのたびにネットワーク５０１を介してデータベースサーバ５０３に権限の照会を行うので、計算機コストを消費することになる。また、ネットワーク５０１に照会データがそのまま送信されるのでセキュリティ上問題がないわけではなかった。

【０００６】

また、上述の問題を回避するためにデータベースサーバ５０３の権限情報のセットまたはサブセットのコピー（データベースサーバ）をウェブ・サーバ５００のサイトにローカルに配置することも考えられる。しかし、このようにすると、データベースサーバ５０３およびそのコピーとの間で一貫性を維持しなければならず、保守管理等が煩雑となる。また、各サイトにデータベースサーバを配置するとコストアップになる。

【０００７】

【発明が解決する課題】

この発明は、以上の事情を考慮してなされたものであり、証明書のサブジェクト名から直ちにその権限や性質を知ることができ、これを用いて簡易にアクセス制御等を行える技術を提供することを目的としている。

【０００８】

【課題を解決するための手段】

この発明によれば、上述の目的を達成するために、特許請求の範囲に記載のと

おりの構成を採用している。ここでは、発明を詳細に説明するのに先だって特許請求の範囲の記載について補充的に説明を行っておく。

【０００９】

この発明の一側面によれば、上述の目的を達成するために、個人証明書に含まれるサブジェクト名を処理する個人証明書サブジェクト名処理装置に：個人証明書を受信する手段と；受信した個人証明書を電子署名技術に基づいて検証する手段と；受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも１つの所定のエレメントを抽出する手段と；上記検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定する手段とを設けるようにしている。

【００１０】

この構成においては、個人証明書を認証してそのサブジェクト名のエレメントの真正を確認し、この真正なエレメントの値に基づいてアクセス権限を判別することができ、ディレクトリサービス等のデータベースにアクセスする必要がなくなる。

【００１１】

この発明の他の側面によれば、上述の目的を達成するために、ウェブ・サーバ・コンピュータ・システムに：個人証明書を受信する手段と；受信した個人証明書を電子署名技術に基づいて検証する手段と；受信した個人証明書に含まれるサブジェクト名の階層中の少なくとも１つの所定のエレメントを抽出する手段と；受信した個人証明書の検証が成功したときに、上記所定のエレメントの値に基づいて、上記個人証明書の保持者のアクセス権限を決定する手段とを設けるようにしている。

【００１２】

この構成においても、ディレクトリサービス等のデータベースを利用することなく簡易にアクセス権限を判別することができる。

【００１３】

ウェブ・サーバ・コンピュータ・システムはウェブ・サーバ単体で構成されてもよく、ウェブ・サーバとアプリケーション・サーバとで構成されてもよい。ア

クセス権限の判別を行うために各種の機能はウェブサーバの認証機能やＣＧＩ（コモンゲートインタフェース）プログラムや、アプリケーション・サーバにより実現される。

【００１４】

この発明のさらに他の側面によれば、上述の目的を達成するために、サブジェクト名の所定のエレメントが保持者の所属組織および個人ＩＤ以外の属性を表す個人証明書を受信して当該サブジェクト名を処理する個人証明書サブジェクト名処理装置に：上記個人証明書を受信する手段と；受信した個人証明書に含まれるサブジェクト名の階層中の所定のエレメントを抽出する手段と；上記所定のエレメントの値が表す、保持者の所属組織および個人ＩＤ以外の属性に基づいて、アクセス権限を決定する手段とを設けるようにしている。

【００１５】

この構成においては、ディレクトリサービス等のデータベースを利用することなく簡易にアクセス権限を判別することができる。とくにサブジェクト名のオーガニゼーショナル・ユニット・ネームを利用することにより柔軟にアクセス権限情報を規定できる。

【００１６】

なお、この発明は装置やシステムとして実現できるのみでなく、方法としても実現できる。またこのような方法の一部をコンピュータプログラムとして実現してもよい。

【００１７】

この発明の上述の各側面およびこの発明の他の側面は特許請求の範囲に記載され、以下、実施例を用いて詳細に説明される。

【００１８】

【発明の実施の形態】

以下、この発明を情報アクセスシステムに適用した実施例について説明する。この実施例は、幹事会社と協力会社とが所定のプロジェクト名の下で協力して事業を行うことを前提とし、幹事会社および協力会社の従業者等が幹事会社の情報にアクセスできるようにするものである。情報のアクセスには個人証明書を利用

する。幹事会社は、個人証明書の発行にイニシャティブを持つ会社（事業体）である。もちろん、この発明は、このような環境下のみでなく、情報をアクセスする際に権限を判別する種々の環境下で適用可能である。上述の幹事会社ではなく、証明書の発行を業とする認証局が、証明書を発行するような環境下でも適用可能である。

【００１９】

図１は、この実施例の情報アクセスシステムを示しており、この図において、証明書発行センタ（幹事会社サイト）１０、協力会社サイト２０等がインターネット３０に接続されている。ここでは、便宜上、証明書発行センタ１０は、幹事会社の社内に設けられているものとする。協力会社サイト２０は、構内ネットワーク網（ＬＡＮ）等によりイントラネットを構築しており、各イントラネットにクライアント端末２０１が接続されている。

【００２０】

この例において、証明書発行センタ１０は、協力会社サイト２０のクライアント端末２０１等からの個人証明書発行申請を受け取って個人証明書の発行処理を行うものである。個人証明書はＩＴＵ－Ｔ勧告Ｘ．５０９に準拠するものであり、図２に示すようなものである。

【００２１】

証明書発行センタ１０は、ウェブ・サーバ１０１、アプリケーション・サーバ１０２、データベース管理システム１０３、メールサーバ１０４、クライアント端末１０５、ルータ１０６等を有している。これらコンピュータリソースはＬＡＮ１０７に接続されている。

【００２２】

ウェブ・サーバ１０１は、ＨＴＴＰ（ハイパーテキストトランスファプロトコル）プロトコルに従ってクライアント（クライアント端末２０１、１０５）から要求を受け取り、要求に応じたＨＴＭＬ文書（ＸＭＬ文書）をクライアントに転送する。アプリケーション・サーバ１０２は、ウェブ・サーバ１０１を介してクライアントから送られたプログラム名および引数に基づいて種々の処理を実行するものである。アプリケーション・サーバ１０２にかえてウェブ・サーバ１０１

のＣＧＩ（コモンゲートインタフェース）のプログラム等を用いてもよい。データベース管理システム１０３は、証明書発行に関連する種々のデータベースを管理するものである。データベースは、例えば、証明書データベース１０３ａ等である。

【００２３】

データベース管理システム１０３が管理する証明書データベース１０３ａに保持される証明書情報の簡略化した例を図３に示す。ここでは、証明書情報について説明する前に、この例で用いるＤＮ（ディスティングイシュトネーム、以下サブジェクト名とも呼ぶ。Ｘ．５０１）について説明しておく。この例では、サブジェクト名は、カントリネーム（Ｃ）、オーガニゼーションネーム（Ｏ）、第１オーガニゼーショナルユニットネーム（ＯＵ１）、第２オーガニゼーショナルユニットネーム（ＯＵ２）、第３オーガニゼーショナルユニットネーム（ＯＵ３）、コモンネーム（ＣＮ）により規定される。幹事会社以外の申請者に対してはＯＵ１として例えば「Ｐａｒｔｎｅｒ」等が記述される。幹事会社の社員については、ＯＵ１を省略したり、ＯＵ１として所定の部門名が記述される。ＯＵ２は、プロジェクト名が記述される。ただしプロジェクトと関係がない場合にはＯＵ２は省略される。ＯＵ３は、協力会社の会社名が記述される。もちろん、幹事会社の内部の者（社員等）に関してはＯＵ３は省略される。このようにして、サブジェクト名を用いてプロジェクトおよび協力会社を記述することができる。なお、ＯＵのサフィックスは、ＯＵの属性に対応して用いており、例えば部門（社外の組織）をあらわすＯＵ１は、部門の階層に応じてさらに階層的な構成を採用してもよい。例えば、「ｊｉｎｊｉ」（人事部）、「ｊｉｎｊｉ１」（第１人事課）等、ＯＵ１を複数規定できる。

【００２４】

なお、プロジェクトとは一括りに管理される業務や活動であり、ここでは便宜上、幹事会社と他の協力会社との間で行われる業務を指す。プロジェクトとの関連で協力会社が登録される。もちろん、幹事会社内のプロジェクトや非業務的な活動等を「プロジェクト」として扱ってもよい。このようにすることにより組織構成から離れて証明書を発行することが可能となる。

【００２５】

サブジェクト名の具体例を説明する。

【００２６】

（１）具体例１

[Ｃ＝ＪＰ，Ｏ＝ＸＹＺ　Ｃｏ．，ＣＮ＝１２３４　Ｒｙｕ　Ｉｎａｄａ]

この例では、保持者がＸＹＺ株式会社の社員であり、社員番号が１２３４で、指名が「Ｒｙｕ　Ｉｎａｄａ」であることがわかる。

【００２７】

（２）具体例２

[Ｃ＝ＪＰ，Ｏ＝ＸＹＺ　Ｃｏ．，ＯＵ＝Ｐａｒｔｎｅｒ，ＯＵ＝Ｘｎｅｔ，ＯＵ＝ＡＢＣ　Ｃｏ．，ＣＮ＝１２３４　００１　Ｔａｒｏ　Ｆｕｊｉ]

この例では、保持者は協力会社のＡＢＣ株式会社の社員であり、プロジェクトＸｎｅｔに参画し、その業務目的が調達（コモンネームの００１が調達を意味する）であり、所属会社の社員番号が１２３４で、氏名が「Ｔａｒｏ　Ｆｕｊｉ」であることがわかる。

【００２８】

（３）具体例３

[Ｃ＝ＪＰ，Ｏ＝ＸＹＺ　Ｃｏ．，ＯＵ＝Ｐａｒｔｎｅｒ，ＯＵ＝Ｘｎｅｔ，ＣＮ＝１２３４　Ｈａｎａｋｏ　Ｆｕｊｉ]

この例では、保持者が派遣社員であり、その派遣社員番号が１２３４であり、氏名が「Ｈａｎａｋｏ　Ｆｕｊｉ」であることを示す。協力会社名あるいはプロジェクト名がないことから派遣社員と判断することができる。

【００２９】

図１の説明に戻る。データベース管理システム１０３が管理する証明書データベース１０３ａは、図３に示すように、証明書情報を保持している。図３に示すように、サブジェクト名は（Ｃ，Ｏ，ＯＵ１，ＯＵ２，ＯＵ３，ＣＮ）であり、コモンネームＣＮは、例えばＣＮ＝１２３４５　００１　Ｔａｒｏ　Ｙａｍａｄａである。「１２３４５」は協力会社ＡＢＣ内の一意の識別子例えば社員番号である。「００１」は幹事会社での業務の種別を示すＩＤである（例えば、調達業

務、試作業務）。「ＴａｒｏＹａｍａｄａ］は申請者の氏名である。証明書データベース１０３ａは証明書ＩＤ、サブジェクト名（Ｃ，Ｏ，ＯＵ１，ＯＵ２，ＯＵ３，ＣＮ）、有効期限等を保持している。なお、証明書は、サブジェクト名、発行者名、公開鍵、発行者署名等を含むものである。

【００３０】

ウェブ・サーバ１０１、アプリケーション・サーバ１０２、データベース管理システム１０３を用いて具体的な証明書発行処理の機能が実現される。クライアントはウェブ・ベースで証明書発行システムの各種の機能を利用できる。

【００３１】

メールサーバ１０４はＳＭＴＰ（シンプルメールトランスファプロトコル）デーモン等を実行するものであり、メールの配送を行なう。

【００３２】

クライアント端末１０５は、ウェブ・ブラウザを具備し、証明書発行センタ（幹事会社）１０内で証明書発行センタ１０のサービスの提供を受ける。

【００３３】

クライアント端末２０１は、協力会社サイト２０に配置されたパーソナルコンピュータ、ワークステーション等であり、ウェブ・ブラウザを実装している。クライアント端末２０１は、証明書発行センタ１０が提供する証明書発行システムにアクセスし、雛型登録（会社登録）、個人証明書発行申請等を行なうことができる。証明書発行センタ１０はインターネット３０上に公開されているため、適宜ファイヤーウォール等のセキュリティ機構が設けられることが望ましい。証明書の発行自体はこの発明と直接には関係がないので、詳細な説明は省略する。通常の証明書発行所理を採用できることはもちろんである。

【００３４】

このような証明書発行センタ１０を用いて証明書の発行を申請し、申請が承認され、証明書が発行される。申請者は、証明書ＩＤを通知され、ウェブ・ベースでこれを入力して証明書を取得する。

【００３５】

つぎに証明書を利用したアクセス制御について説明する。

【００３６】

図４はアクセス制御を行う機構を模式的に示すものである。この機構はウェブ・サーバ１０１、アプリケーション・サーバ１０２により実現される。もちろん、ウェブ・サーバ１０１のＣＧＩプログラムや、ＪＡＶＡサーブレット（商標）等を用いてアプリケーション・サーバ１０２に代替させることができる。

【００３７】

図４において、セクセス制御機構は、ルート証明書保持部１５０、認証部１５１、エレメント抽出部１５２、権限判別部１５３、権限登録部１５４、セッション管理部１５５等を含んで構成される。この例では、ウェブ・サーバ１０１が、ルート証明書保持部１５０および認証部１５１を構成する。そして、アプリケーション・サーバ１０２がエレメント抽出部１５２、権限判別部１５３、権限登録部１５４、セッション管理部１５５を構成する。

【００３８】

認証部１５１は図５に示すような認証手続をクライアント端末およびウェブ・サーバ１０１間で実現する。図５の認証手続は通常のＳＳＬ／ＴＬＳコネクション要求時にウェブ・サーバ１０１で実行される認証手続であり、図から明らかであるのでとくに説明は行わない。認証部１５１は、この認証手続の際に、クライアント端末から証明書を受け取る。この証明書は図５に示す認証手続に利用されるとともに、そのサブジェクト名がエレメント抽出部１５２に供給される。認証部１５１は、ルート証明書保持部１５０に保持されているルート証明書の公開鍵を用いて、クライアント端末から受け取った証明書の署名（図２参照）を検証する。検証が失敗したときにはコネクションは拒否される。検証が成功すると、セッション番号（セッションＩＤともいう）が割り当てられ、アプリケーション・サーバ１０５のセッション管理部１５５によりセッション変数が記憶管理される管理される。

【００３９】

エレメント抽出部１５２はサブジェクト名の階層構造を辿って所定のエレメントを抽出する。この例では、ＯＵ１が「Ｐａｒｔｎｅｒ」であり、ＯＵ３に会社名がある場合に、ＯＵ２のプロジェクト名、ＯＵ３の会社名、ＣＮの業務種別コ

ード（例えば「００１」）を抽出する。

【００４０】

権限判別部１５３は図６に示すような区別に従って文書のアクセス権限を決定し、これをセッション番号に割り当てる。図６に示す区別は例えば図７に示すようなテーブルで実装可能であり、権限判別部１５３がこのようなテーブルを参照して、アクセス可能なファイルやディレクトリを判別する。権限登録部１５４はセッション番号と権限（権限レベルやアクセス可能なファイル名／ディレクトリ名）との関係をセッション管理部１５５に登録する。例えば、セッション管理部１５５のデータベース（図示しない）に図８に示すように登録する。以降、セッションが継続する間、このセッション番号に基づいてアクセス権限が許容される。

【００４１】

なお、以上の認証手続や権限制御は、証明書発行センタ（幹事会社サイト）１０のウェブ・サーバ１０１との間でのみ可能なわけではなく、他のウェブ・サーバとの間でも可能であり、また、同様の認証手続や権限制御をその他種々のサーバとの間で実行できることはもちろんである。

【００４２】

上述の実施例では、証明書発行センタ１０が幹事会社サイトに設けられるようにしたが、図９に示すように、証明書発行センタ１０と幹事会社サイト４０とを個別に設けてもよいことはもちろんである。図９に示す例では、証明書発行の機能を証明書発行センタ１０に割り当て、ウェブベースでサービスを行う機能を幹事会社サイト４０に設けている。幹事会社サイト４０には上述実施例と同様な権限制御をウェブ・サーバ１０１で実行する。図９の例ではウェブ・サーバ１０１自体が認証部１５１およびルート証明書保持部１５０を構成し、ウェブ・サーバ１０１のＣＧＩプログラムがエレメント抽出部１５２、権限判別部１５３、権限登録部１５４、セッション管理部１５５を構成している。ＣＧＩプログラムでなくＪＡＶＡサーブレット等を用いてもよい。もちろん、図１に示すようなアプリケーション・サーバを用いてもよい。

【００４３】

図９においては図１と対応する箇所に対応する符号を付し、説明を繰り返さない。

【００４４】

また、上述では、幹事会社と協力会社とが協力してプロジェクトを行う環境を例に挙げて説明を行ったが、任意の形態のサーバとクライアントとの間の権限制御を同様に行えることはもちろんである。

【００４５】

以上説明したようにこの発明によれば個人証明書のサブジェクト名を利用して簡易に保持者の権限や性質を判別でき、簡易にアクセス制御を行うことができる。

【００４６】

すなわち、従来ディレクトリサービスサーバ（データベースサーバ）で管理していたアクセス制限に関する情報を、サブジェクト名の中に、そのオーガニゼーショナル・ユニット・ネームやコモンネームの一部として埋め込み、その内容の真正を証明書の署名により確認した上で利用させることができ、ディレクトリサーバ等を用いることなくアクセス制限の情報をサーバに供給することが可能になる。サーバ側では、サブジェクト名に埋め込まれた情報と権限との関係を記述したテーブル等を保持するだけで簡易にアクセス権限を知ることができる。

【００４７】

この結果、ディレクトリサーバを用いてアクセス制限を行っていた従来システムの欠点を解消することができる。すなわち、サブジェクト名や権限レベルがネットワーク（例えばインターネット）上を行き交うことがなくなり、また、ディレクトリサーバ等のコピーを各サーバのサイトに配置する必要もなくなる。

【００４８】

なお、この発明は上述の実施例に限定されるものではなくその趣旨を逸脱しない範囲で種々変更が可能である。例えば、上述例では、コモンネームに業務種別のコードを含ませたが、所定階層のオーガニゼーショナル・ユニット・ネームに含ませても良い。また、この発明のサブジェクト名の構成をアクセス制御以外の用途に用いることもできることは明らかである。

【００４９】

【発明の効果】

以上説明したように、この発明によれば、個人証明書を用いて簡易にアクセス制御等を行うことができる。

【図面の簡単な説明】

【図１】　この発明の実施例を全体として示すシステム図である。

【図２】　上述の実施例で用いる個人証明書を説明する図である。

【図３】　上述実施例の証明書データベースを説明する図である。

【図４】　上述実施例の申請者権限の制御を模式的に説明するブロック図である。

【図５】　上述実施例の認証手続を説明する図である。

【図６】　上述実施例の権限の区別を説明する図である。

【図７】　上述実施例の権限の区別を規定するテーブルの例を説明する図である。

【図８】　上述実施例のセッション管理を説明する図である。

【図９】　上述実施例の変形例を説明する図である。

【図１０】　従来例を説明する図である。

【符号の説明】

１０　　証明書発行センタ

２０　　協力会社サイト

３０　　インターネット

４０　　幹事会社サイト

１０１　　ウェブ・サーバ

１０２　　アプリケーション・サーバ

１０３　　データベース管理システム

１０３ａ　　証明書データベース

１０４　　メールサーバ

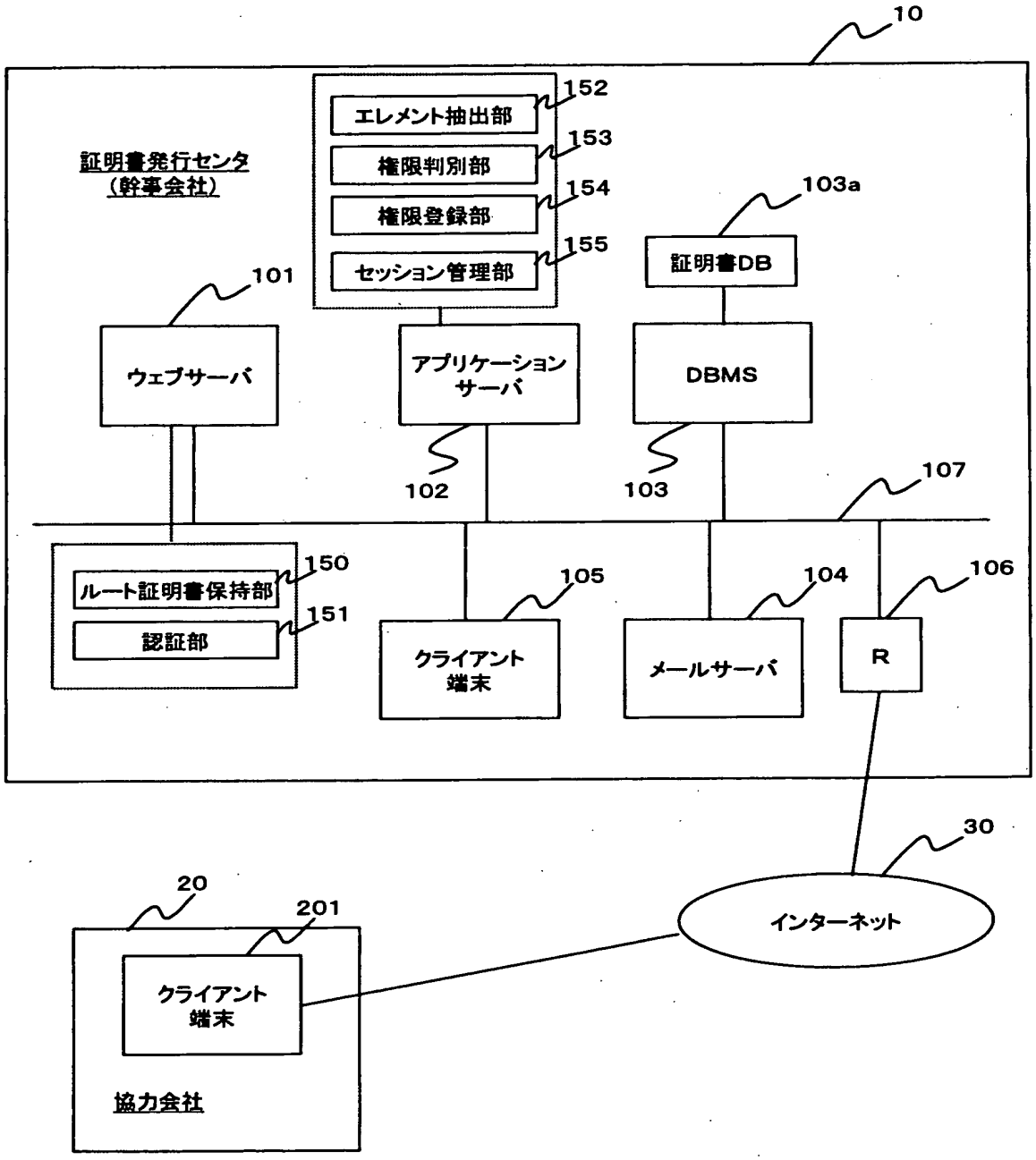
１０５　　アプリケーション・サーバ

１０５　　クライアント端末

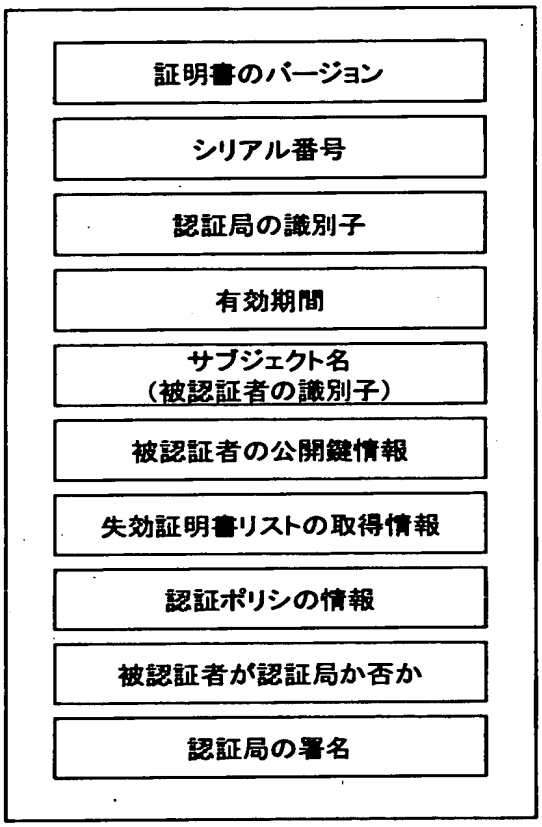
１０６	ルータ
１５０	ルート証明書保持部
１５１	認証部
１５２	エレメント抽出部
１５３	権限判別部
１５４	権限登録部
１５５	セッション管理部
２０１	クライアント端末
５００	クライアント端末
５０１	ネットワーク
５０２	ウェブ・サーバ
５０３	データベースサーバ

【書類名】　　図面

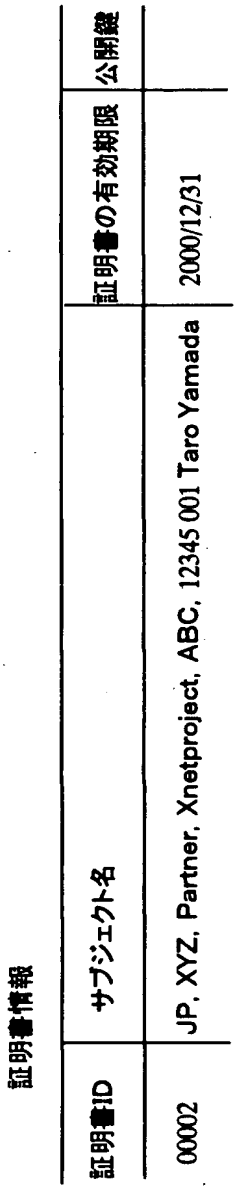
【図１】


10
証明書発行センタ
（幹事会社）
エレメント抽出部
152
権限判別部
153
権限登録部
154
セッション管理部
155
103a
証明書DB
101
ウェブサーバ
アプリケーション
サーバ
DBMS
102
103
107
ルート証明書保持部
150
認証部
151
105
クライアント
端末
104
メールサーバ
106
R
30
インターネット
20
201
クライアント
端末
協力会社

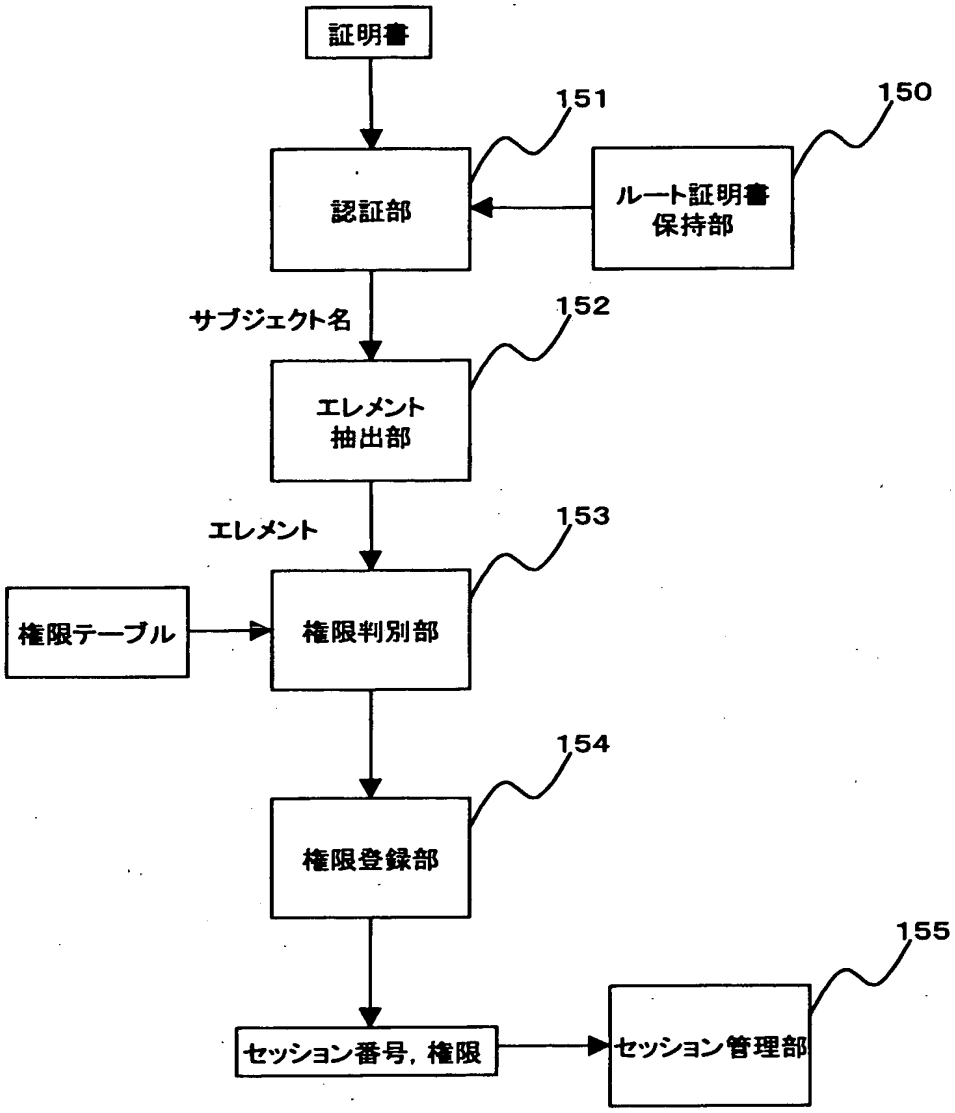
【図２】


証明書のバージョン
シリアル番号
認証局の識別子
有効期間
サブジェクト名
（被認証者の識別子）
被認証者の公開鍵情報
失効証明書リストの取得情報
認証ポリシの情報
被認証者が認証局か否か
認証局の署名

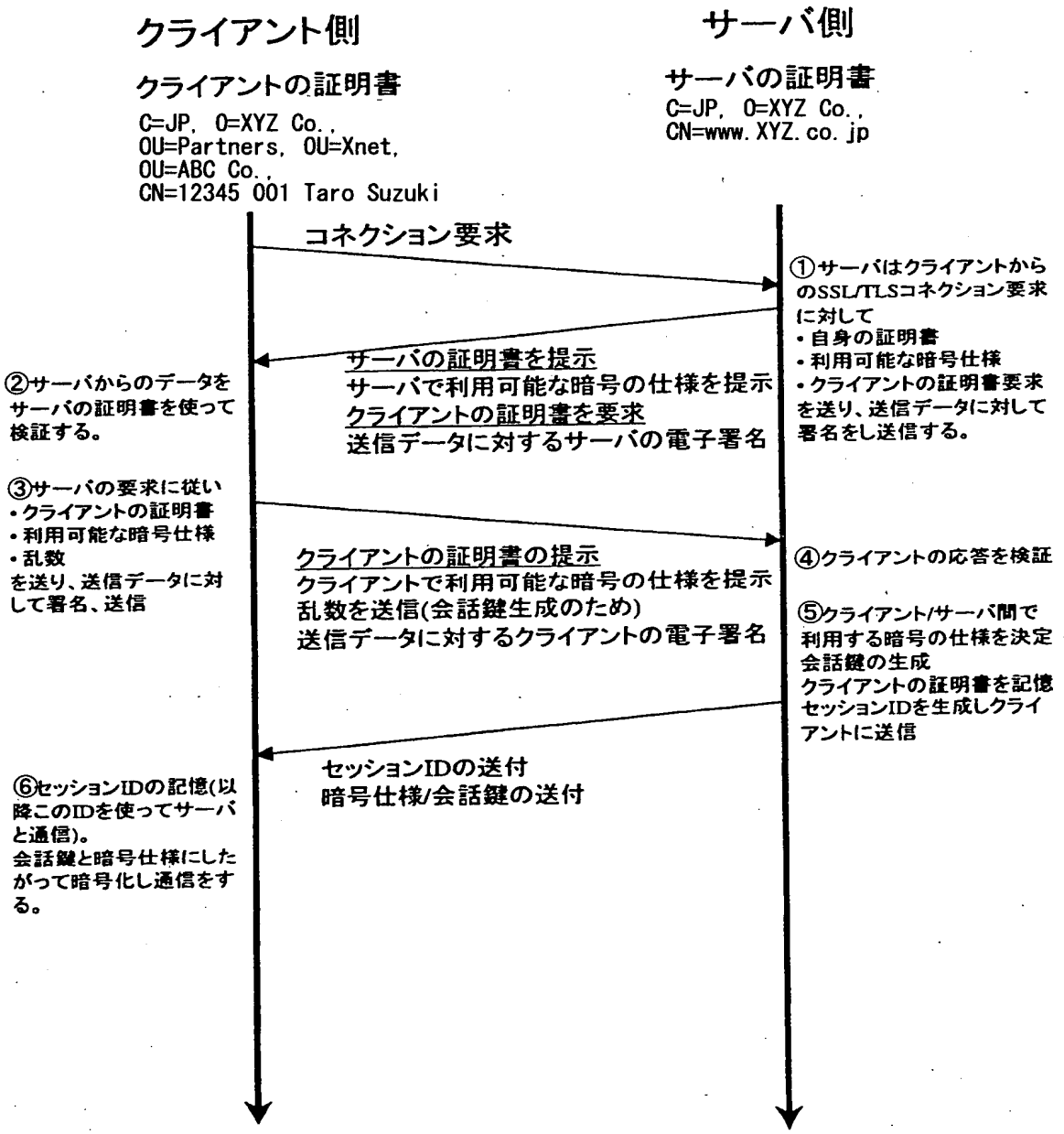
【図３】


証明書情報
証明書ID
サブジェクト名
証明書の有効期限
公開鍵
00002
JP, XYZ, Partner, Xnetproject, ABC, 12345 001 Taro Yamada
2000/12/31

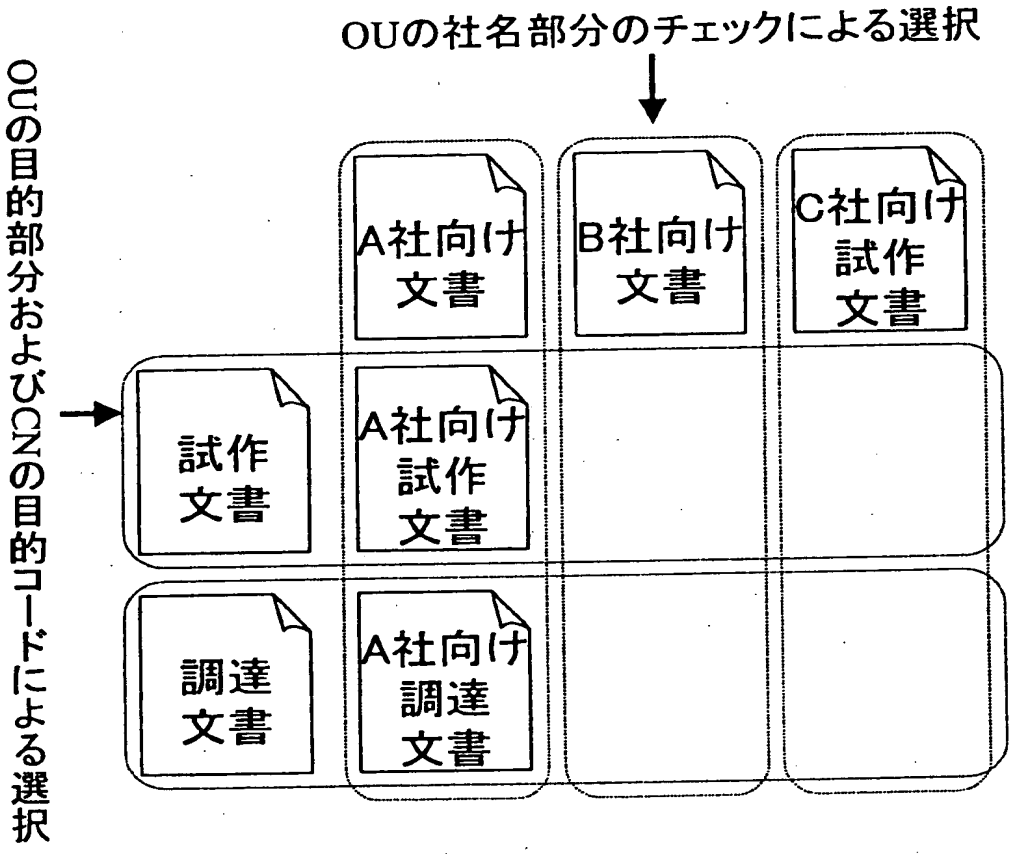
【図４】


証明書
151
150
認証部
ルート証明書
保持部
サブジェクト名
152
エレメント
抽出部
エレメント
153
権限テーブル
権限判別部
154
権限登録部
155
セッション番号，権限
セッション管理部

【図５】


クライアント側
クライアントの証明書
C=JP, O=XYZ Co.,
OU=Partners, OU=Xnet,
OU=ABC Co.,
CN=12345 001 Taro Suzuki
サーバ側
サーバの証明書
C=JP, O=XYZ Co.,
CN=www.XYZ.co.jp
コネクション要求
①サーバはクライアントからのSSL/TLSコネクション要求に対して
・自身の証明書
・利用可能な暗号仕様
・クライアントの証明書要求
を送り、送信データに対して署名をし送信する。
サーバの証明書を提示
サーバで利用可能な暗号の仕様を提示
クライアントの証明書を要求
送信データに対するサーバの電子署名
②サーバからのデータをサーバの証明書を使って検証する。
③サーバの要求に従い
・クライアントの証明書
・利用可能な暗号仕様
・乱数
を送り、送信データに対して署名、送信
クライアントの証明書の提示
クライアントで利用可能な暗号の仕様を提示
乱数を送信(会話鍵生成のため)
送信データに対するクライアントの電子署名
④クライアントの応答を検証
⑤クライアント/サーバ間で利用する暗号の仕様を決定
会話鍵の生成
クライアントの証明書を記憶
セッションIDを生成しクライアントに送信
セッションIDの送付
暗号仕様/会話鍵の送付
⑥セッションIDの記憶(以降このIDを使ってサーバと通信)。
会話鍵と暗号仕様にしたがって暗号化し通信をする。

【図６】


OUの社名部分のチェックによる選択
OUの目的部分およびCNの目的コードによる選択
A社向け文書
B社向け文書
C社向け試作文書
試作文書
A社向け試作文書
調達文書
A社向け調達文書

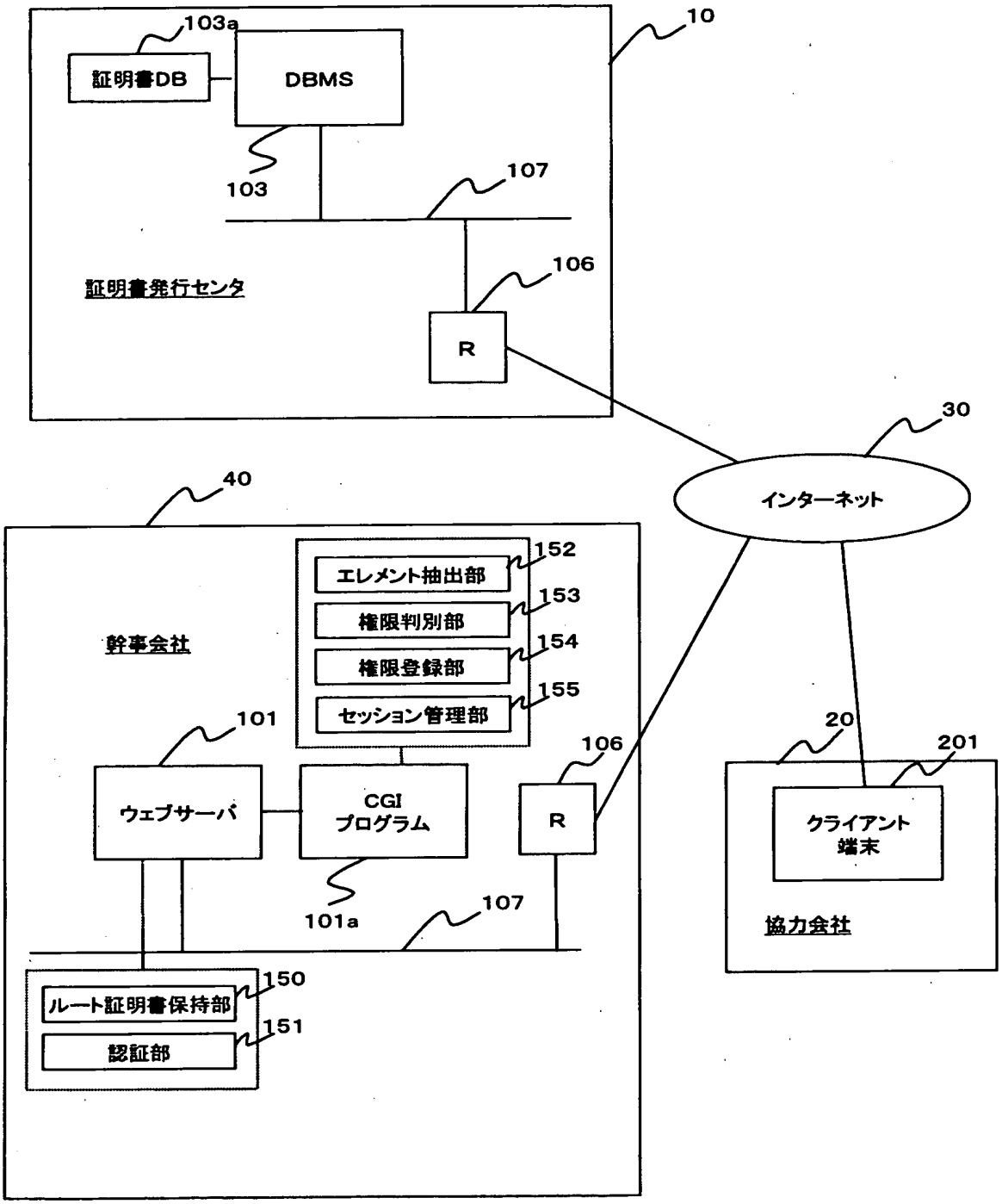
【図７】

プロジェクト	目的コード	ファイル名／ディレクトリ名

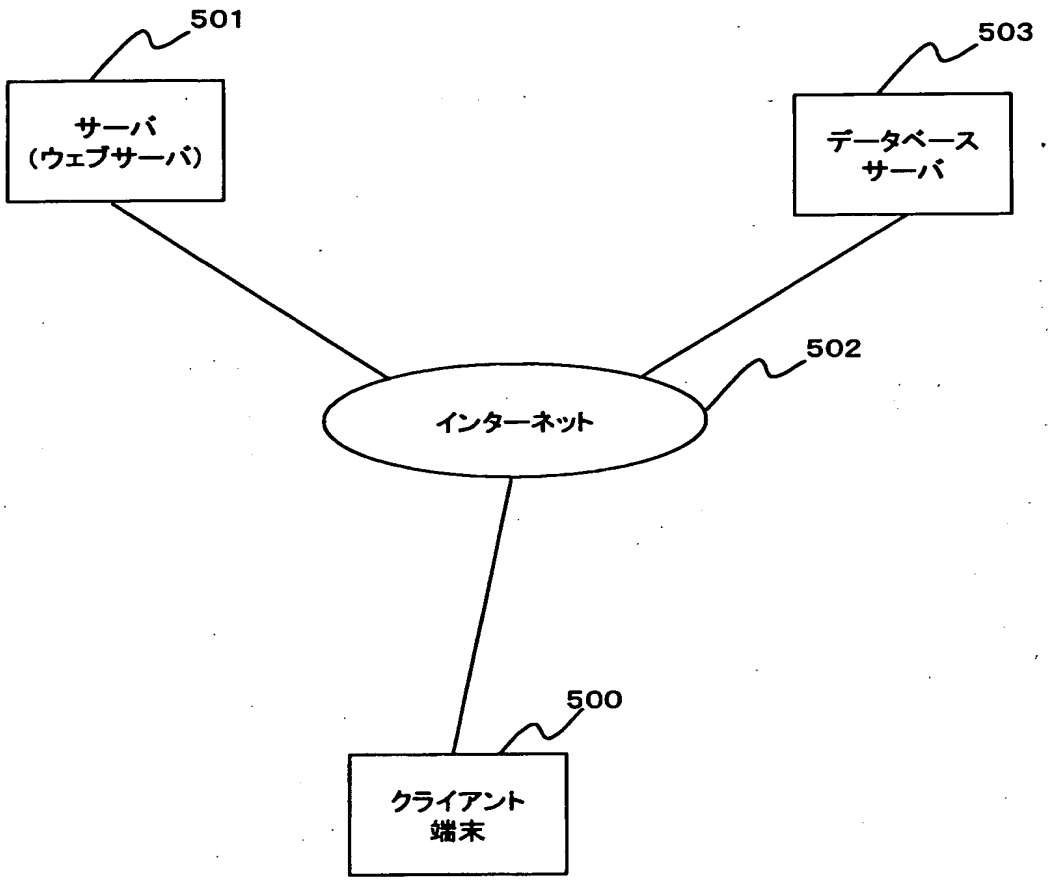
【図８】

セッション番号	権限（アクセス可能ファイル名／ディレクトリ名）

【図９】


103a
証明書DB
DBMS
10
103
107
106
証明書発行センタ
R
30
インターネット
40
152
エレメント抽出部
153
権限判別部
154
権限登録部
155
セッション管理部
幹事会社
101
106
20
201
ウェブサーバ
CGI
プログラム
R
クライアント
端末
101a
107
協力会社
150
ルート証明書保持部
151
認証部

【図１０】



【書類名】　要約書

【要約】

【課題】　証明書のサブジェクト名を利用して簡易にアクセス制御等を行う。

【解決手段】　認証部１５１は認証手続をクライアント端末２０１およびウェブサーバ１０１間で実現する。認証部１５１は、この認証手続の際に、クライアント端末から証明書を受け取り、そのサブジェクト名がエレメント抽出部１５２に供給される。エレメント抽出部１５２はサブジェクト名の階層構造を辿って所定のエレメントを抽出する。権限判別部１５３は抽出したエレメントの種類、値に基づいて文書のアクセス権限を決定し、これをセッション番号に割り当てる。権限登録部１５４はセッション番号と権限との関係を登録し以降、セッションが継続する間、このセッション番号に基づいてアクセス権限が許容される。

【選択図】　図４

出　願　人　履　歴　情　報

識別番号　　〔０００００５４９６〕

１．変更年月日　　１９９６年　５月２９日
［変更理由］　住所変更
住　所　東京都港区赤坂二丁目１７番２２号
氏　名　富士ゼロックス株式会社